(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－302008

(43)公開日　平成10年(1998)11月13日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	17/60		Ｇ０６Ｆ	15/21	３３０
	5/00			5/00	Ｚ
	15/00	３３０		15/00	３３０Ｚ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ａ
					６０１Ｅ

審査請求　未請求　請求項の数５　ＦＤ　（全 20 頁）　最終頁に続く

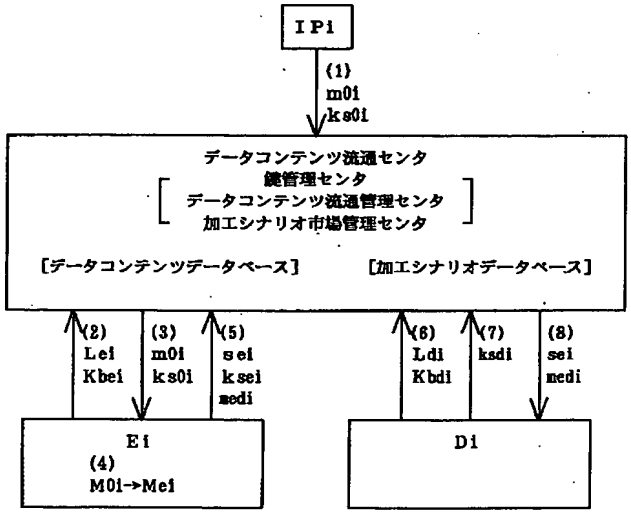
(21)出願番号　特願平9－126357

(22)出願日　平成９年(1997)４月30日

(71)出願人　000005979
三菱商事株式会社
東京都千代田区丸の内２丁目６番３号
(72)発明者　斉藤　誠
東京都千代田区丸の内二丁目６番３号　三菱商事株式会社内
(74)代理人　弁理士　南條　眞一郎

(54)【発明の名称】　データコンテンツ流通システム

(57)【要約】
【発明の課題】　原データコンテンツ及び加工データコンテンツを流通させるためのシステムを提供する。
【解決手段】　データコンテンツとしてオブジェクトを取り扱い、データコンテンツの加工はオブジェクトであるデータコンテンツを加工プログラムによって加工することによって行われ、加工データコンテンツは原データコンテンツと加工プログラムによる加工内容を記載した加工シナリオとによって表現される。流通するのは暗号化された加工シナリオのみであり、暗号化加工シナリオを入手したユーザは鍵管理センタから入手した暗号鍵を用いて暗号化加工シナリオを復号し、加工シナリオに従ってデータベースから原データコンテンツを入手し加工データコンテンツを再構成する。加工シナリオの販売を希望する者がいる場合には、競売を行い加工シナリオの使用権を販売する。



1

【特許請求の範囲】

【請求項１】　データベースに保存されている原データコンテンツ及び前記原データコンテンツを第１ユーザが加工した加工データコンテンツをネットワーク上で第２ユーザに販売するデータコンテンツ流通システムであって：前記データコンテンツ流通システムでは、

前記原データコンテンツが、データオブジェクトで構成され；前記加工データコンテンツが、前記データオブジェクトと前記データオブジェクトの加工内容を記載した加工シナリオから構成され；前記データコンテンツ流通システムが、データコンテンツ流通センタとデータベースから構成され；前記データコンテンツ流通センタが、鍵管理センタ，データコンテンツ流通管理センタ及び加工シナリオ流通管理センタから構成され；前記鍵管理センタが、秘密鍵生成，秘密鍵保管及び秘密鍵配送を行い；前記データコンテンツ流通管理センタが、前記データベースに保存されているデータコンテンツの広告及び販売を行い；前記加工シナリオ流通管理センタが、前記加工シナリオの広告及び販売を行い；前記第１ユーザが、前記データベースに保存されている原データコンテンツを利用して加工データコンテンツを作成し、該加工データコンテンツの加工シナリオを秘密鍵で暗号化して前記データベースに預託するとともに該秘密鍵を前記鍵管理センタに預託し；該暗号化加工シナリオ及び該秘密鍵が該加工データコンテンツの利用を希望する第２ユーザに配送され；該第２ユーザが該秘密鍵を用いて該暗号化加工シナリオ復号し、該復号された加工シナリオに基づいて該加工データコンテンツを再構成するデータコンテンツ流通システム。

【請求項２】　前記データベースが、データコンテンツを保存するデータコンテンツデータベースと加工シナリオを保存する加工シナリオデータベースから構成されている請求項１のデータコンテンツ流通システム。

【請求項３】　該原データコンテンツが該暗号化加工シナリオ及び該秘密鍵とともに第２ユーザに配送される請求項１のデータコンテンツ流通システム。

【請求項４】　データベースに保存されている前記原データコンテンツをデータコンテンツ加工者が加工した加工シナリオをネットワーク上でデータコンテンツ販売者に競売により売却するデータコンテンツ流通システムであって：前記データコンテンツ流通システムでは、

前記原データコンテンツが、データオブジェクトで構成され；前記加工データコンテンツが、前記データオブジェクトと前記データオブジェクトの加工内容を記載した加工シナリオから構成され；前記データコンテンツ流通システムが、データコンテンツ流通センタとデータベースから構成され；前記データコンテンツ流通センタが、鍵管理センタ，データコンテンツ流通管理センタ及び加工シナリオ流通管理センタから構成され；前記鍵管理センタが、秘密鍵生成，秘密鍵保管及び秘密鍵配送を行い；前記データコンテンツ流通管理センタが、前記データベースに保存されている前記データコンテンツの広告及び販売を行い；前記加工シナリオ流通管理センタが、前記加工シナリオの広告及び競売を行い；前記データコンテンツ加工者が、前記データベースに保存されている原データコンテンツを利用して加工データコンテンツを作成し、該加工データコンテンツの加工シナリオを前記データコンテンツ加工者の秘密鍵で暗号化して前記データベースに預託するとともに該秘密鍵を前記鍵管理センタに預託し；該加工シナリオの販売を希望する加工シナリオ販売者に競売を行い；該加工シナリオ販売者が該加工シナリオ用の秘密鍵を鍵管理センタにに転送し；前記加工シナリオ流通管理センタが該加工シナリオ用の秘密鍵を前記データコンテンツ加工者の秘密鍵から該加工シナリオ販売者の秘密鍵に変更するデータコンテンツ流通システム。

【請求項５】　前記データベースが、データコンテンツを保存するデータコンテンツデータベースと加工シナリオを保存する加工シナリオデータベースから構成されている請求項４のデータコンテンツ流通システム。

【発明の詳細な説明】

【０００１】

【技術分野】本発明は著作権デジタルデータコンテンツの流通、即ち、原デジタルデータコンテンツ及び加工されたデジタルデータコンテンツの流通における著作権管理システムに係るものである。

【０００２】

【従来技術】アナログデータコンテンツは保存，複写，加工，転送をする毎に品質が劣化するために、これらの作業によって生じる著作権の処理は大きな問題とはならなかった。しかし、デジタルデータコンテンツは保存，複写，加工，転送を繰り返して行っても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。これまで、デジタルデータコンテンツの著作権処理には的確な方法がなく、著作権法であるいは契約で処理されており、著作権法においてもデジタル方式の録音・録画機器に対する補償金が制度化されているにすぎない。

【０００３】データコンテンツの利用法は単にその内容を参照するだけでなく、通常は得たデータコンテンツを保存，複写，加工することによってユーザが有効活用し、ユーザが加工したデータコンテンツを通信回線を経由してオンラインであるいは適当な記憶媒体を利用してオフラインで他人に転送したりさらにはデータベースに対して転送し、新しいデータコンテンツとして登録することさえ可能であり、その場合にはデータコンテンツを加工したユーザも新たな情報提供者になることができる。

【０００４】このような状況において、データベース化されたデータコンテンツの著作権をどのように取扱うか

が大きな問題となるが、これまでのところそのための著作権管理手段、特に、複写，加工，転送等の２次利用について完成された著作権管理手段はない。本発明者らは特開平６－４６４１９号（ＧＢ２２６９３０２Ａ）及び特開平６－１４１０００４号（ＵＳＰ５５０４９３３）で公衆電信電話回線を通じて鍵管理センタから許可鍵を入手することによって著作権管理を行うシステムを、特開平６－１３２９１６号（ＧＢ２２７２８２２Ａ）でそのための装置を提案した。

【０００５】また、特開平７－２７１８６５・ＥＰ６７７９４９Ａ２（ＵＳ０８／４１６０３７）において、これらの上記先願発明をさらに発展させることによって、デジタル映像のリアルタイム送信も含むデータベースシステムにおけるデジタルデータコンテンツの表示（音声化を含む），保存等の１次利用及び複写，加工，転送等の２次利用における著作権管理方法を提案した。

【０００６】この先願のデータベース著作権管理システムでは、著作権の管理を行うために、申し込まれた利用形態に対応した利用許可鍵の他に、著作権を管理するためのプログラム，著作権情報あるいは著作権管理メッセージの何れか一つあるいは複数を用い、暗号化して転送されたデータコンテンツを復号して、視聴・加工の利用を行い、保存・複写・転送の利用を行う場合にデータコンテンツは再暗号化される。

【０００７】著作権管理メッセージは申し込みあるいは許可内容に反する利用が行われようとした場合に画面に表示され、ユーザに対して注意あるいは警告を行い、著作権管理プログラムはデータコンテンツの復号化／暗号化を行うとともに申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【０００８】また、本発明者らは具体的なデータベース著作権管理システムを特開平８－１８５４４８・ＥＰ７０４７８５Ａ２（ＵＳ０８／５３６７４７）において提案した。このシステムは、データベース著作権管理システムを、暗号鍵を管理する鍵管理センタ及びデータベース著作権を管理する著作権管理センタから構成し、データベースから配布されるデータコンテンツは全て第１の暗号鍵によって暗号化(encrypt)され、データベースから直接にデータを利用する第１ユーザは、鍵管理センタに対して第１ユーザの情報を提示して利用形態に対応する鍵の要求を行い、第１ユーザから１次利用申込を受けた鍵管理センタは第１ユーザの情報を著作権管理センタに転送し、第１ユーザの情報を受け取った著作権管理センタはこの情報とともに著作権管理プログラムを鍵管理センタに転送し、著作権管理プログラムを受け取った鍵管理センタは著作権管理プログラムと利用形態に対応する第１の暗号鍵(crypt key)、第２の暗号鍵を第１ユーザに対して通信ネットワークを経由して転送し、第１の暗号鍵を受け取った第１ユーザは受け取った第１の暗号鍵を用いてデータを復号(decrypt)して利用し、以後データの保存、コピーあるいは転送を行う場合には第２の暗号鍵を用いて暗号化及び復号化が行われる。

【０００９】データコンテンツが保存されずに外部記憶媒体にコピーされたときあるいは転送されたときには第１暗号鍵及び第２暗号鍵は廃棄され、第１ユーザが再度データコンテンツを利用する場合には著作権管理センタから第１暗号鍵と第２暗号鍵の再交付を受け、この第２暗号鍵の再交付を受けたことにより、第２ユーザへのデータコンテンツのコピーあるいは転送が行われたことが確認され、このことが著作権管理センタに記録される。

【００１０】第２ユーザは著作権管理センタへの２次利用申込のときに第１ユーザの情報及び原著作権についての情報を著作権管理センタに提示する。著作権管理センタは利用形態に対応する許可鍵とともに暗号化された第２暗号鍵（視聴許可鍵）及び第３暗号鍵（利用形態に対応した許可鍵）及び著作権管理プログラムを第２ユーザに送信する。

【００１１】一方、企業内等の組織においてコンピュータを相互に接続してＬＡＮ（LocalArea Network）を構成することが広く行われているが、複数のネットワークを相互に接続し、複数のネットワーク全体をあたかも１つのネットワークであるかのように利用するインターネット（Internet）が世界的な規模で構成されている。

【００１２】企業内等の組織内のＬＡＮには組織外に知られてはならない秘密情報が保管されていることが多い。そのため、そのような秘密情報は特定のユーザのみが利用できるようにする必要があり、外部への秘密情報の漏洩を防止するために、一般的にはアクセスコントロールが行われる。アクセスコントロール方法には、大きく分けてアクセス許可によって行う方法と、暗号化によって行う方法の２種類の方法がある。

【００１３】アクセス許可によるアクセスコントロール方法は、ＵＳＰ５１７３９３９，５２２０６０４，５２２４１６３，５３１５６５７，５４１４７７２，５４３８５０８，ＥＰ５０６４３５，ＪＰ開６２－１６９５４０に述べられている。暗号化によるアクセスコントロール方法は、ＵＳＰ４７３６４２２，５２２４１６３，５４００４０３，５４５７７４６，５５８４０２３，ＥＰ４３８１５４，５０６４３５，ＪＰ開５－１４５９２３に述べられており、暗号化とデジタル署名によるアクセスコントロール方法が、ＵＳＰ４９１９５４５，５４６５２９９に述べられている。

【００１４】また、複数のＬＡＮをインターネットを経由して接続しあたかも単一のＬＡＮであるかのように利用するイントラネット（Intranet）が普及しつつある。このイントラネットにおいては本質的に窃取等に対する安全性を有しないインターネットを経由して情報交換を行うため、秘密情報を交換する場合には窃取防止のために情報の暗号化が行われる。伝送時の情報窃取を暗号化により防止することが、ＵＳＰ５５０４８１８，５５１

５４４１に述べられており、その場合に複数の暗号鍵を用いることがＵＳＰ５５０４８１６，５３５３３５１，５４７５７５７及び５３８１４８０に述べられており、再暗号化を行うことがＵＳＰ５４７９５１４に述べられている。

【００１５】暗号化する場合には、暗号鍵の受け渡しを含む暗号鍵管理が重要な問題となるが、暗号鍵生成をＩＣカードによって行うことがＵＳＰ５５７７１２１に、暗号化／復号化をＩＣカードによって行うことがＵＳＰ５３４７５８１，５５０４８１７に各々述べられている。また、電子透かし技術がＥＰ６４９０７４に述べられている。

【００１６】ところで、コンピュータネットワークシステムの発展に伴い従来はスタンドアローンで使用されていた個々のコンピュータがネットワークシステムを介して接続され、データを共有するデータベースシステムが普及し、データだけでなくアプリケーションプログラム、さらにはオペレーティングシステムと呼ばれる基本ソフトウェアまでもネットワークを介して共有する分散オブジェクトシステムも提案されている。

【００１７】分散オブジェクトシステムは、データコンテンツもソフトウェアもともにプログラムとデータからなるオブジェクトとして、サーバから供給される。分散オブジェクトシステムには、オペレーティングシステム，アプリケーションプログラム及びデータコンテンツはサーバが提供し、データコンテンツ処理及びデータコンテンツ保存は通常のコンピュータであるユーザ端末装置で行うオブジェクトコンテナと呼ばれるシステムと、オペレーティングシステム，アプリケーションプログラム及びデータはサーバが提供し、データ処理はネットワークコンピュータと呼ばれるユーザ端末装置が行うがデータコンテンツの保存はサーバが行うシステムがある。このシステムはさらに押し進めて、データコンテンツ処理もサーバが行い、ユーザ端末装置は入出力の機能のみしか有せず、システム全体が一つのコンピュータとして機能するものまでが考えられている。

【００１８】一方、データヘッダとデータボディから構成される通常の形式のファイルの代わりに、データコンテンツとデータコンテンツを扱うプログラムとが一体化された「オブジェクト」を用いて種々の処理を行う「オブジェクト指向プログラミング(object oriented progr aming)」がある。オブジェクトはインスタンス(instanc e)と呼ばれる容器(envelope)中のスロット(slot)と呼ばれる格納箇所にインスタンス変数(instance variable)と呼ばれるデータが格納され、スロットの周囲は参照(r efering)用，加工(processing)用，結合(binding)用等の１個又は複数のメソッド(method)と呼ばれる手続きで包囲されており、インスタンス変数を参照したり操作したりすることはメソッドを介してしか行うことはできず、この機能は隠蔽(encapsulation)と呼ばれる。ま

た、インスタンス変数の参照あるいは操作をメソッドに行わせる外部からの命令をメッセージと呼ぶ。

【００１９】このことは見方を変えると、メソッドを介さなければ参照あるいは操作することができないインスタンス変数はメソッドによって保護されていることになる。このことを利用し、メソッドを暗号化し、暗号化されたメソッドを復号できるメッセージでなければインスタンス変数を参照あるいは操作することができないようにすることができる。この場合も通常のファイル形式を有するデータの場合と同様にメソッドの全てを暗号化してしまうとオブジェクトを利用することができなくなるため、メソッドの一部を暗号化しない。

【００２０】また、ネットワークシステムの別の形態として、通信回線等のネットワーク基盤を提供する事業者が通信回線以外の課金システム、セキュリティシステム、著作権管理システム、認証システム等を提供し、サービス事業者がこれらのシステムサービスを利用してあたかも自己のシステムのようにしてネットワーク事業を行うライセンスネットワークと呼ばれる「賃貸ネットワークシステム」も構想されている。

【００２１】先行技術の最後に本発明で利用する基本的な暗号関連技術について説明する。

［暗号鍵］秘密鍵(secret key)システムは暗号化と復号化が同じ鍵で行れるため「共通鍵システム」とも呼ばれ、鍵を秘密にしておく必要があることから「秘密鍵システム」と呼ばれる。秘密鍵を用いる暗号アルゴリズムとして代表的なものに米国標準局(National Bureau of Standards)のＤＥＳ(Data Encryption Standard)システム，日本電信電話のＦＥＡＬ(Fast Encryption Algorithm)システム，三菱電機のＭＩＳＴＹシステムがある。以下説明する実施例において秘密鍵を「Ks」と表示する。

【００２２】これに対して公開鍵システムは、公開されている公開鍵(puBlic key)とその鍵の所有者以外には秘密にされている専用鍵(priVate key)を用い、一方の鍵で暗号化し他方の鍵で復号化する暗号システムであり、代表的なものにＲＳＡ公開鍵システムがある。本明細書では公開鍵を「Kb」と、専用鍵を「Kv」と表示する。このときに、平文データコンテンツＭ(Material)を秘密鍵Ksを用いた暗号文Cmks(Cryptogram)に暗号化(Encryption)する操作を、

Cmks＝Ｅ（Ｍ，Ks）

暗号文Cmksを暗号鍵Ksを用いて平文データコンテンツＭに復号化(Decryption)する操作を、

Ｍ＝Ｄ（Cmks，Ks）

また、平文データコンテンツＭを公開鍵Kbを用いて暗号文Cmkbに暗号化する操作を、

Cmkb＝Ｅ（Ｍ，Kb）

暗号文Cmkbを専用鍵Kvを用いて平文データコンテンツＭに復号化する操作を、

M＝D（Cmkv，Kv）
と、平文データコンテンツMを専用鍵Kvを用いて暗号文Cmkvに暗号化する操作を、
Cmkv＝E（M，Kv）
暗号文Ckvを公開鍵Kbを用いて平文データコンテンツMに復号化する操作を、
M＝D（Cmkb，Kb）
と表現する。

【００２３】暗号技術はデータコンテンツの不正利用を不可能にするための手段であるが、その動作が完璧であるとの保証はないため、不正利用の可能性を完全に否定することができない。一方、電子透かし技術は不正利用を不可能にすることはできないが、不正利用が発見されたときには、電子透かしの内容を検証することにより不正利用であることを確定することができるが手段であり、種々の方法があるが日経エレクトロニクス６８３号，ｐ．９９～１２４に「「電子透かし」がマルチメディア時代を守る」（１９９７／２／２４，日経ＢＰ社刊）に全般的に紹介されており、また同号，ｐ．１４９～１６２，ウォルター　ベンダー他「電子透かしを支えるデータ・ハイディング技術（上）」及び６８４号，ｐ．１５５～１６８，「電子透かしを支えるデータ・ハイディング技術（下）」（IBM System Journal，vol.35，nos.3 & 4(International Business Machines Corporation)から転載）にも紹介されている。

【００２４】

【発明の概要】本出願においては原データコンテンツ及び加工データコンテンツを流通させるためのシステムについて提案する。本出願において取り扱われるデータコンテンツはオブジェクトであり、データコンテンツの加工はオブジェクトであるデータコンテンツを加工プログラムによって加工することによって行われ、加工データコンテンツは原データコンテンツと加工プログラムによる加工内容を記載した加工シナリオとによって表現される。利用される原データコンテンツにはデータベースに保存されているものの他にデータ加工者が作成したものがあるが、データ加工者が作成したデータコンテンツもデータベースに保存することにより他のデータと同様に取り扱われる。流通するのは暗号化された加工シナリオのみであり、暗号化加工シナリオを入手したユーザは鍵管理センタから入手した暗号鍵を用いて暗号化加工シナリオを復号し、加工シナリオに従ってデータベースから原データコンテンツを入手し加工データコンテンツを再構成する。加工シナリオの販売を希望する者がいる場合には、競売により使用権を販売する。

【００２５】

【実施例】図を参照しながら最適実施例を説明する。データコンテンツの加工は、原著作物データをアプリケーションプログラムである加工ツールを用いて編集することによって行われ、加工によって得られた加工データコンテンツは、利用した原データコンテンツ，使用した加工ツールの情報及び加工内容データとによって表現することができる。すなわち、加工ツールを所有している場合には、原著作物データと加工内容データを入手することにより、加工著作物データを再現することが可能である。

【００２６】初めに、デジタルデータの加工について説明する。デジタルデータの加工は加工用プログラム（加工ツール）を利用して原データコンテンツに改変を加えることによってなされるため、原データコンテンツ、加工ツール及び加工内容データ（加工シナリオ）が特定されることによって加工データコンテンツが再現される。いいかえれば、原データコンテンツ、加工ツールと加工シナリオが特定されなければ加工データコンテンツの再現は不可能である。

【００２７】単一の原データコンテンツにより新しいデータコンテンツを作成する場合には、原データコンテンツＡを改変して加工データコンテンツ「Ａ’」を得る場合、原データコンテンツＡにユーザがデータコンテンツＸを付加することにより加工データコンテンツ「Ａ＋Ｘ」を得る場合、原データコンテンツＡを原データコンテンツ要素Ａ1，Ａ2，Ａ3・・・に分割し配列をＡ3，Ａ2，Ａ1のように変更して加工データコンテンツ「Ａ”」を得る場合、原データコンテンツＡを原データコンテンツ要素Ａ1，Ａ2，Ａ3・・・に分割し第１ユーザのデータコンテンツＸをＸ1，Ｘ2，Ｘ3・・・に分割しこれらを配列して加工データコンテンツ「Ａ1＋Ｘ1＋Ａ2＋Ｘ2＋Ａ3＋Ｘ3・・・」を得る場合等がある。これらの場合、原データの改変、原データコンテンツの配列変更、原データコンテンツとユーザデータコンテンツの組み合わせ、原データコンテンツの分割及びユーザデータコンテンツとの組み合わせ、が各々二次著作権の対象となり、これらの二次著作権を保護する必要がある。なお、ユーザが付加したデータコンテンツＸにはユーザの原著作権が存在することはいうまでもない。

【００２８】複数の原データコンテンツを組み合わせることにより新しいデータコンテンツを作成する場合には、原データコンテンツＡ，Ｂ，Ｃ・・・を単純に組み合わせて加工データコンテンツ「Ａ＋Ｂ＋Ｃ・・・」を得る場合、原データコンテンツＡ，Ｂ，Ｃ・・・にユーザがデータコンテンツＸを付加することにより加工データコンテンツ「Ａ＋Ｘ」を得る場合、原データコンテンツＡ，Ｂ，Ｃ・・・を原データコンテンツ要素Ａ1，Ａ2，Ａ3・・・，Ｂ1，Ｂ2，Ｂ3・・・，Ｃ1，Ｃ2，Ｃ3・・・に分割し組み合わせて配列を変更し加工データコンテンツ「Ａ1＋Ｂ1＋Ｃ1＋・・・＋Ａ2＋Ｂ2＋Ｃ2＋・・・＋Ａ3＋Ｂ3＋Ｃ3＋・・・」を得る場合、原データコンテンツＡ，Ｂ，Ｃ・・・を原データコンテンツ要素Ａ1，Ａ2，Ａ3・・・，Ｂ1，Ｂ2，Ｂ3・・・，Ｃ1，Ｃ2，Ｃ3・・・に分割しユーザのデータコンテンツＸ1，Ｘ

2，X3・・・を組み合わせて配列を変更して加工データコンテンツ「A1＋B1＋C1＋X1＋・・・＋A2＋B2＋C2＋X2＋・・・＋A3＋B3＋C3＋X3＋・・・」を得る場合等がある。これらの場合も、複数の原データコンテンツの組み合わせ、複数の原データコンテンツとユーザデータコンテンツの組み合わせ、複数の原データコンテンツの分割及び配列変更、分割された複数の原データコンテンツとユーザデータコンテンツの組み合わせ、が各々２次的著作権の対象となり、これらの２次的著作権を保護する必要がある。また、ユーザが付加したデータコンテンツX1，X2，X3・・・にはユーザの原著作権が存在することはいうまでもない。

【００２９】図面を用いて実施例１を説明する。図１に示されたのは、ユーザが１つの原著作物データを加工して、次のユーザに転送するデータ著作権管理システムの構成図である。この実施例において、１，２，３はテキストデータ，コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ，音声データあるいは映像データが暗号化されずに格納されたデータベースであり、９は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するＣＡＴＶ回線等の通信回線、１０はフレキシブルディスク等の記録媒体、４は第１ユーザ端末装置、５は第２ユーザ端末装置、６は第３ユーザ端末装置、７はｎ次ユーザ端末装置である。また、８はデータ著作権を管理する著作権管理センタである。

【００３０】これらのうちデータベース１，２，３、著作権管理センタ８、第１ユーザ端末装置４、第２ユーザ端末装置５、第３ユーザ端末装置６及びｎ次ユーザ端末装置７は通信回線９に接続されている。この図において、破線で示された経路は暗号化されたデータコンテンツが伝送される経路であり、実線で示された経路は各ユーザ端末装置４，５，６，７から各データベース１，２，３及び著作権管理センタ８への要求が伝送される経路であり、１点鎖線で示された経路は各データベース１，２，３及び著作権管理センタ８から各ユーザ端末装置４，５，６，７へ利用形態に対応する許可鍵、著作権管理プログラム及び暗号鍵が送信される経路である。

【００３１】本実施例１においては、第１ユーザが用意する第１公開鍵Kb1，第１公開鍵Kb1に対応する第１専用鍵Kv1，第２公開鍵Kb2，第２公開鍵Kb2に対応する第２専用鍵Kv2，データベースが用意する第１秘密鍵Ks1，第２秘密鍵Ks2が使用される。データベースでは、データコンテンツMを第１秘密鍵Ks1を用いて暗号化し、

Cmks1＝E（M，Ks1）

第１秘密鍵Ks1を第１公開鍵Kb1を用いて暗号化する

Cks1kb1＝E（Ks1，Kb1）

とともに第２秘密鍵Ks2を第２公開鍵Kb2を用いて暗号化し、

Cks2kb2＝E（Ks2，Kb2）

これらの暗号化データコンテンツCmks1，暗号化第１秘密鍵Cks1kb1及び暗号化第２秘密鍵Cks2kb2を第１ユーザに送信する。

【００３２】第１ユーザ側では、暗号化第１秘密鍵Cks1kb1を第１専用鍵Kv1を用いて復号し、

Ks1＝D（Kv1，Cks1kb1）

復号された第１秘密鍵Ks1を用いて暗号化データコンテンツCmls1を復号して

M＝D（Ks1，Cmks1）

利用するとともに、暗号化第２秘密鍵Cks2kb2を第２専用鍵Kv2を用いて復号し、

Ks2＝D（Kv2，Cks2kb2）

復号された第２秘密鍵Ks2は以降におけるデータコンテンツの保存・複写・転送時の暗号／復号鍵として使用される。

【００３３】第１ユーザが入手したデータコンテンツをそのまま複写して第２ユーザに供給した場合にはそのデータコンテンツに何等の変更も加えられていないため、そのデータコンテンツに第１ユーザの著作権は発生しない。しかし、第１ユーザが入手したデータコンテンツを基に新しいデータコンテンツを作成した場合あるいは他のデータコンテンツと組み合わせる等の手段を用いて新しいデータコンテンツを作成した場合にはその新しいデータコンテンツについて第１ユーザの２次著作権が発生し、この第１ユーザはその２次著作物の著作権者になる。同様に、第２ユーザが第１ユーザから入手したデータコンテンツを基に新しいデータコンテンツを作成した場合あるいは他のデータコンテンツと組み合わせる等の手段を用いてさらに新しいデータを作成した場合には、同様にその新しいデータコンテンツについて第２ユーザの２次著作権が発生し、この第２ユーザはその２次著作物の著作権者になる。

【００３４】各データベース１，２，３にはテキストデータコンテンツ，コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータコンテンツ，ディジタル音声データコンテンツ，ディジタル映像データコンテンツが格納されており、第１ユーザ端末装置４からの要求に対してデータコンテンツ読み出し時に暗号化された状態で通信回線９を経由して第１ユーザ端末装置４に供給される。

【００３５】データベースから入手するデータ著作権の管理は先願である特願平６－２３７６７３（特開平８－１８５４４８，US０８／５３６７４７，EP７０４７８５A２）に記載されている方法あるいは本件出願と同時に提出する出願に記載されている方法で行われる。

【００３６】図２に示されたように、第１ユーザは単一のデータベースからあるいは複数のデータベースから入手した複数の原データコンテンツM1，M2，M3からデータコンテンツを構成するパーツM4，M5，M6を抽出

し、これらのパーツM4，M5，M6を利用して新しいデータコンテンツM7を生成する。

【００３７】このように生成された新しいデータコンテンツM7を第１ユーザは第２ユーザ５に供給するが、新しいデータコンテンツM7には第１ユーザが原データコンテンツM1，M2，M3を加工することによって発生した２次的著作権の他に、データコンテンツM7を生成するための原料であるパーツM4，M5，M6を得た原データコンテンツM1，M2，M3についての原著作権も存在している。

【００３８】これらの各原データコンテンツM1，M2，M3は表示以外の利用すなわち保存，加工，複写あるいは転送が行われるときには各データコンテンツとともに供給された各第２秘密鍵Ks21，Ks22，Ks23で暗号化されるが、

Cm1ks21＝E（M1，Ks21）

Cm2ks22＝E（M2，Ks22）

Cm3ks23＝E（M3，Ks23）

各々の原データコンテンツの部品M4，M5，M6も同様に表示以外の利用が行われるときには各原データコンテンツとともに供給された第２秘密鍵Ks21，Ks22，Ks23で暗号化される。

Cm4ks21＝E（M4，Ks21）

Cm5ks22＝E（M5，Ks22）

Cm6ks23＝E（M6，Ks23）

【００３９】データ加工者である第１ユーザ４は加工プログラムPeに第１専用鍵Kv1を用いてデジタル署名を行い、

Spe＝D（Pe，Kv1）

デジタル署名された加工プログラムPeとともに暗号化原データ部品Cm4ks21，Cm5ks22，Cm6ks23を通信回線９を経由してあるいは記録媒体１０に記録して第２ユーザ５に供給する。

【００４０】デジタル署名された加工プログラムPeとともに暗号化原データコンテンツ部品Cm4ks21，Cm5ks22，Cm6ks23を受け取った第２ユーザは、著作権管理センタ８に対してデジタル署名が行われた加工プログラムPeを提示して暗号化原データコンテンツ部品Cm4ks21，Cm5ks22，Cm6ks23を復号するための第２秘密鍵Ks21，Ks22，Ks23を要求する。

【００４１】著作権管理センタ８は、第１公開鍵Kb1を用いて提示された加工プログラムのデジタル署名から第１ユーザ４を確認し、

Pe＝E（Spe，Kb1）

その第１ユーザが第２秘密鍵Ks21，Ks22，Ks23を要求された原データコンテンツの正当な利用者であることを確認し、その第１ユーザが正当な利用者である場合には第２秘密鍵Ks21，Ks22，Ks23を第２ユーザに転送する。しかし、その第１ユーザが正当な利用者でない場合には第２の秘密鍵Ks21，Ks22，Ks23を第２ユーザに転送しない。

【００４２】著作権管理センタに提示されたデジタル署名Speは第１ユーザが２次的著作権者であることを証明する正式な手続きとして著作権管理センタに登録される。

【００４３】このデータの加工は原データコンテンツをその原データコンテンツに対応する加工プログラムを使用して加工することもできるが、原データコンテンツをオブジェクト指向ソフトウェアとして取り扱うようにすれば、より容易な加工とよりよいデータ著作権管理を行うことができる。また、さらに進んでエージェント指向ソフトウェアを採用すれば、ユーザは労することなくデータコンテンツの合成を行うことができる。

【００４４】エージェント指向ソフトウェアは、自律性・適応性・協調性を兼ね備えたプログラムであり、従来のソフトウェアのようにすべての作業手順を具体的に指示しなくても、ユーザの一般的な指示のみに基づいてその自律性・適応性・協調性との特質により、ユーザの要求に応えることができる。このエージェントプログラムをデータ著作権管理システムの基本的なシステムの中に組み込み、ユーザのデータベース利用形態を監視させ、ユーザ端末装置に装備されたメータリング機能を利用して利用データ明細、課金情報などを含む情報をデータベース側あるいは著作権管理センタ側で収集するように構成することにより、ユーザのデータベース利用傾向をデータベース側あるいは著作権管理センタ側が知ることができ、よりきめの細かい著作権管理を行うことができる。したがって、エージェントプログラム及びデータも著作権保護の対象となり、原データコンテンツと同様に暗号化される。

【００４５】著作権データはプログラムとデータコンテンツが一体化した「オブジェクト」としてコンピュータプログラミングあるいは各種処理において部品的な取り扱いをすることができる。

【００４６】図３により実施例２を説明する。この実施例においては第１秘密鍵Ks1，第２秘密鍵Ks2，第３秘密鍵Ks3，平文である原著作権ラベルLc0及び平文である著作権管理プログラムPcが用いられる。図３に示されたデータ著作権管理システムは、データベース１１、鍵管理センタ１２、ユーザ１３，１３，１３・・・およびこれらを相互に接続する通信回線１４から構成されている。また、データベース１１には情報提供者（Information Provider：ＩＰ）１５，１５，１５・・・からデータコンテンツが供給されるが、場合によってはデータベース１１を経由することなく情報提供者１６，１６，１６・・・から通信回線１４を経由して直接にユーザ１３に対してデータコンテンツが供給されることがある。なお、本発明において利用されるデータコンテンツはプログラムとデータが組み合わされたオブジェクトである。また、データベース１１には情報提供者１５，１

５，１５・・・から第１ユーザ１３にデータコンテンツが供給されるが、場合によっては情報提供者１６，１６，１６・・・からネットワーク１４を経由してあるいはＣＤＲＯＭ等の情報記録媒体１７を介してデータベース１１を経由することなく直接に第１ユーザ１３に対してデータコンテンツが供給されることもある。なお、この図において実線で示されたのは平文データ及び暗号鍵要求の経路、破線で示されたのは暗号化データコンテンツの経路、１点鎖線で示されたのは暗号鍵の経路である。第１ユーザ１３は単なる利用者ではなく入手した複数の原データコンテンツを組み合わせたり、修正したりすることにより新しい著作物（２次著作物）を提供する情報提供者１５あるいは１６となりうる。

【００４７】このデータ著作権管理システムにおいて、各情報提供者１５，１６から提供される原データコンテンツは著作権を保護するために暗号化されている。したがって、第１ユーザ１３が入手した暗号化原データコンテンツを利用するには暗号化原データコンテンツを復号化しなければならない。このシステムにおいてはそのための暗号鍵はすべて鍵管理センタ１２に預けられ、鍵管理センタ１２が管理する。なお、各情報提供者１５，１６が採用する暗号方式は自由であるが、後で述べる２次利用以降で使用される暗号方式は鍵管理センタ１２が採用する方式に限られる。

【００４８】このシステムにおいて、平文である原データコンテンツM0は第１秘密鍵Ks1を用いて暗号化され、

Cm0ks1＝E（M0，Ks1）

原著作権ラベルLc0とともに情報提供者１５からデータベース１１を介してネットワーク１４を経由して、情報提供者１６から通信回線１４を経由してあるいはＣＤＲＯＭ等の情報記録媒体１７を介して第１ユーザ１３に供給される。

【００４９】第１ユーザ１３に供給される暗号化原データコンテンツCm0ks1には平文の原著作権ラベルLc0が付けられており、平文の原著作権ラベルLc0は１次利用鍵の入手等に利用される。すなわち、暗号化原データコンテンツCm0ks1は平文原著作権ラベルLc0と暗号化原データコンテンツCm0ks1から構成されている。平文原著作権ラベルLc0には原データコンテンツの原著作者名，タイトル名，制作日等の一般情報の他に、使用しているアプリケーション・プログラム名，概要説明，使用料金及び課金方法等が記載されており、さらに必要に応じて暗号鍵の番号が記載されている。なお、平文原著作権ラベルLc0に原著作権者によるデジタル署名を付しておけば虚偽の申告を防止することができる。

【００５０】供給された暗号化原データコンテンツCm0ks1の利用を希望する第１ユーザ１３は、ネットワーク１４を経由して鍵管理センタ１２に原著作権ラベルLc0を提示して１次利用鍵K1の配布を要求する。

【００５１】提示された原著作権ラベルLc0により、配布すべき秘密鍵が第１秘密鍵Ks1であることを確認した鍵管理センタ１２は確認された第１秘密鍵Ks1をネットワークシステム１４を経由して第１ユーザ１３に配布する。配布された１次利用鍵K1を受信した時点で第１ユーザ１３の装置は著作権管理モードになり、第１ユーザ１３は１次著作権データコンテンツの利用が可能になる。一方、鍵管理センタ１２は課金処理を行うとともに原データコンテンツの使用状況および第１ユーザ１３のデータベース利用状況を把握する。

【００５２】第１ユーザ１３は配布された第１秘密鍵Ks1を用いて暗号化原データコンテンツCm0ks1を復号し、

M0＝D（Cm0ks1，Ks1）

利用する。復号された原データコンテンツM0が第１ユーザ１３の装置内に保存される場合には第１秘密鍵Ks1を用いて再暗号化され、

Cm0ks1＝E（M0，Ks1）

再暗号化原データCm0ks1が保存される。再暗号化された原データコンテンツCm0ks1を再利用する場合には第１秘密鍵Ks1を用いて再復号化及び再暗号化が行われる。

【００５３】原著作権データM0の加工を希望する第１ユーザ１３はネットワーク１４を経由して鍵管理センタ１２に第２秘密鍵Ks2の配布を要求する。

【００５４】第２秘密鍵Ks2の配布要求を受けた鍵管理センタ１２は、ネットワーク１４を経由して第２秘密鍵Ks2を第１ユーザ１３に配布する。第２秘密鍵Ks2を受け取った第１ユーザ１３は原データコンテンツM0の加工を行い、途中加工データM0’を得る。途中加工データコンテンツM0’がユーザ１３の装置内に保存される場合には、第２秘密鍵Ks2によって暗号化される。

Cm0’ks2＝E（M0’，Ks2）

加工が最終的に終了すると、第１ユーザ１３は最終加工データコンテンツM1についてのデータ加工に関する２次著作権を行使するために第３秘密鍵Ks3を用意し、第３秘密鍵Ks3を鍵管理センタ１２に登録する。なお、第３秘密鍵Ks3は第１ユーザ１３ではなく鍵管理センタ１２が用意し、第１ユーザ１３からの要求により配布するようにしてもよい。

【００５５】第１ユーザ１３が加工データコンテンツM1を外部記憶媒体１８への複写あるいはネットワーク１４を介して転送する場合には、第３秘密鍵Ks3を用いて暗号化し、

Cm1ks3＝E（Ks3，M1）

第２ユーザ１９へ供給する。

【００５６】供給された暗号化加工データコンテンツCm1ks3の利用を希望する第２ユーザ１９は、鍵管理センタ１２に通信回線１４を経由して第３秘密鍵Ks3の配布を要求する。第２ユーザ１９からの第３秘密鍵Ks3の配

布要求を受けた鍵管理センタ１２は、通信回線１４を経由して第３秘密鍵Ks3を第２ユーザ１９に配布する。第３秘密鍵Ks3を受け取った第２ユーザ１９は、第３秘密鍵Ks3を用いて暗号化加工データコンテンツCm1ks3を復号化し、

M1＝D（Ks3，Cm1ks3）

利用する。その場合も、暗号化データコンテンツCm1ks3を再度利用する場合には第３秘密鍵Ks3を用いて復号化および暗号化が行われる。

【００５７】［実施例３］ユーザが１つの原著作物データを加工して、次のユーザに転送する実施例３を図４により説明する。

【００５８】この実施例において、データコンテンツの著作権を保護し、データ著作権を行使するために「ユーザラベル」、「著作権ラベル」及び「加工ラベル」が使用される。ユーザラベルにはラベル所有者の情報が記載されている。「著作権ラベル」には原著作物に関する情報が記載されている。「加工ラベル」には原著作権データに関する情報，加工ツールの情報及び加工データ（加工シナリオ）が記載されており、加工ツール情報の代わりに加工ツール（加工プログラム）を記載することもできる。

【００５９】ユーザラベルはユーザがシステムに加入するときにユーザの情報に基づきデータ管理センタにより生成され、著作権ラベルは著作を行った著作者がデータ管理センタにその内容を提示することによりデータ管理センタによって生成され、加工ラベルはデータコンテンツの加工を行ったユーザがユーザラベルと加工シナリオをデータ管理センタに提示することによりデータ管理センタによって作成され、これらは各々のラベル所有者に転送されるとともに、データ管理センタ内に保存される。

【００６０】(1) 原著作者（データ所有者）Aは、原著作権ラベルL0を提示して、原秘密鍵Ks0の配布を、データ管理センタに要求する。なお、原著作者が、情報提供業者あるいはデータベースに原データコンテンツを譲渡あるいは管理預託しておき、情報提供業者あるいはデータベースが原著作者の役割を果たすようにすることもできる。また、原著作者Aが原秘密鍵Ks0を保管し、データ管理センタに依存することなく原データコンテンツM0の暗号化を行うことも可能であるが、ユーザ（データ利用者）による原データコンテンツM0の利用を行うためにはデータ管理センタに原秘密鍵Ks0が保管されている必要がある。

【００６１】(2) 原秘密鍵Ks0の配布を要求されたデータ管理センタは、原著作権ラベルLc0とともに原著作権ラベルLc0に対応させた原秘密鍵Ks0を原著作者Aの公開鍵Kb0を用いて暗号化し、

Cks0kb0＝E（Ks0，Kb0）

暗号化原秘密鍵Cks0kb0を、原著作者Aに送付する。

【００６２】データ管理センタは、このときに原著作権ラベルLc0をMD５等のアルゴリズムを用いて一方向ハッシュ、例えば１６バイトのデータ量に、を行い原著作権ラベル指紋F0を作成し、原著作者Aに送付する。この、電子指紋は原データコンテンツあるいは加工が行われ加工データコンテンツが得られる度に各々の加工データコンテンツについて作成され、データコンテンツとともに転送される。

【００６３】(3) 暗号化原秘密鍵Cks0kb0を配付された原著作者Aは、暗号化原秘密鍵Cks0kb0を原著作者Aの専用鍵Kv0を用いて復号し、

Ks0＝D（Cks0kb0，Kv0）

復号された原秘密鍵Ks0を用いて原著作物データコンテンツM0を暗号化し、

Cm0ks0＝E（M0，Ks0）

暗号化原データコンテンツCm0ks0と原著作権ラベルLc0及び原著作権ラベル指紋F0を、第１ユーザU1に転送する。

【００６４】(4) 暗号化原著作物データコンテンツCm0ks0と原著作権ラベルLc0及び原著作権ラベル指紋F0を転送された第１ユーザU1は、原著作権ラベルLc0と原著作権ラベル指紋F0及び第１ユーザラベルLu1を提示して、原秘密鍵Ks0の配布を、データ管理センタに要求する。

【００６５】(5) 原秘密鍵Ks0の配布を要求されたデータ管理センタは、提示された原著作権ラベルL0の正当性を原著作権ラベル指紋F0によって確認して、第１ユーザラベルLu1を登録するとともに、原著作権ラベルLc0に対応する原秘密鍵Ks0を第１ユーザU1の公開鍵Kb1を用いて暗号化して、

Cks0kb1＝E（Ks0，Kb1）

暗号化原秘密鍵Cks0kb1を、第１ユーザU1に配布する。

【００６６】(6) 暗号化原秘密鍵Cks0kb1を配布された第１ユーザU1は、暗号化原秘密鍵Ck0kb1を第１ユーザU1の専用鍵Kv1を用いて復号し、

Ks0＝D（Cks0kb1，Kv1）

復号された原秘密鍵Ks0を用いて暗号化原データコンテンツCm0ks0を復号し、

M0＝D（Cm0ks0，Ks0）

復号された原データコンテンツM0を加工ツールを用いて加工し、加工データコンテンツMe1を得る。

【００６７】このようにして得られた加工データコンテンツMe1にはデータの加工を行った第１ユーザの著作権とともに、原データコンテンツを作成した原著作者の著作権も存在している。原データコンテンツM0に関する原著作者の著作権は登録された原著作権ラベルLc0及び原著作権ラベル指紋F0と原著作権ラベルLc0に対応させた原秘密鍵Ks0、第１ユーザラベルLu1と第１ユーザラベルLu1に対応させた第１秘密鍵Ks1によって保護す

ることができるが、加工データコンテンツMe1を暗号化する鍵は用意されていないため、加工データコンテンツMe1に関する第１ユーザの二次著作権は未だ保護される状態にはなっていない。

【００６８】(7) 加工データコンテンツMe1に関する第１ユーザの二次著作権を保護するために、この実施例においては、加工データコンテンツの著作者である第１ユーザラベルとその電子指紋を利用する。前に説明したように加工著作物は、利用した原データコンテンツ，使用した加工ツールの情報及び加工内容データとによって表現することができるから、第１ユーザラベルいいかえれば第１加工ラベルLe1にはこれらの情報及びデータが記入される。さらに、以後の流通過程における二次著作権保護のために、ユーザU1は第１加工ラベルLe1を、データ管理センタに提示し、このことによってユーザU1の二次著作権の登録が行われる。

【００６９】(8) 第１加工ラベルLe1を提示されたデータ管理センタは、提示された原著作権ラベルLc0の正当性を原著作権ラベル指紋F0によって確認して、第１加工ラベルLe1を登録するとともに、第１加工ラベルLe1の電子指紋F1を作成し、第１加工ラベルLe1に対応させた第１加工秘密鍵Kse1をデータ管理センタの第１ユーザU1の公開鍵Kb1で暗号化し、

Ｃｋse1kb1＝Ｅ（Kse1，Kb1）

暗号化第１加工秘密鍵Ｃｋse1kb1を第１加工ラベルLe1の電子指紋Fe1とともに、第１ユーザU1に送付する。

【００７０】(9) 暗号化第１加工秘密鍵Ｃｋse1kb1及び第１加工著作権ラベルLe1の電子指紋Fe1を配布された第１ユーザU1は、暗号化第１加工秘密鍵Ｃｋse1kb1を第１ユーザU1の専用鍵Kv1を用いて復号し、

Kse1＝Ｄ（Ckse1kb1，Kv1）

復号された第１加工秘密鍵Kse1を用いて第１加工データコンテンツMe1を暗号化し、

Cme1kse1＝Ｅ（Me1，Kse1）

暗号化第１加工データコンテンツCme1kse1を第１加工著作権ラベルLe1及び第１加工著作権ラベルLe1の電子指紋Fe1とともに、第２ユーザU2に転送する。以後、同様な動作が繰り返される。

【００７１】なお、各ユーザが、データ管理センタに提示するそのユーザのラベルにそのラベルの一方向性ハッシュ値をユーザの専用鍵を用いて暗号化したデジタル署名を付け、データ管理センタがそのユーザの公開鍵を用いて暗号化一方向性ハッシュ値を復号し、そのラベルの一方向性ハッシュ値を計算し、両一方向性ハッシュ値を比較することにより、各ユーザラベルの正当性の検証を行うことができる。

【００７２】この実施例において、加工データの転送時に暗号化第１加工データコンテンツCme1kse1とともに転送されるのは第１加工著作権ラベルLe1及び第１加工著作権ラベルLe1の電子指紋Fe1だけであるが、他のラベル及び電子指紋も同時に転送されるように構成することもできる。図２に示されたような複数のデータコンテンツを利用して行う加工はデータコンテンツの数が多い分動作が煩雑であるが、単一データコンテンツを利用した加工の場合と同様にして行われるため、説明が冗長にならないように省略する。

【００７３】以上説明したシステムでは、データコンテンツは秘密鍵を用いて暗号化されており、その復号用秘密鍵及び保存・複写・転送に用いる再暗号化用秘密鍵はユーザが提示したユーザラベルに基づいてデータ管理センタにより配布される。

【００７４】［実施例４］ライセンスネットワークシステムに代表される分散オブジェクトシステムの場合には、大容量のデータ保存装置を有する従来のコンピュータではなく、データ保存装置を有せずデータの入出力及びデータの処理のみを行うネットワークコンピュータの使用が考慮されている。さらには、データ処理機能すら有せずデータの入出力機能のみを有する、大型コンピュータのターミナル装置的なネットワークコンピュータを使用することも考慮されている。このようなネットワークコンピュータはデータ保存装置を有していないため著作物データを保存あるいは複写することはできない。

【００７５】次に、このような分散オブジェクトシステムで使用されるデータ保存装置を有していないネットワークコンピュータに対しても適用可能な実施例を説明するが、この実施例は通常のデータ保存装置を有するコンピュータに対しても適用可能であることは当然のことである。

【００７６】データ著作権を保護するには著作物の無許可利用を制限するために、何らかの暗号技術を使用する必要がある。実施例３では通常のデータ保存装置を有するコンピュータを対象としたシステムでの著作権を保護するために、暗号化されたデータコンテンツと、データコンテンツを利用するための手がかりとして暗号化されていないラベルを用いている。これに対して、ターミナル装置的な機能しか有していないネットワークコンピュータを対象としたシステムにおいては、データコンテンツが保存，複写あるいは転送されることはないためデータコンテンツを暗号化する必要はない。

【００７７】データコンテンツの加工は、原データコンテンツを加工ツールを用いて改変することによって行われ、加工によって得られた加工データコンテンツは、利用した原データコンテンツ，使用した加工ツールの情報及び加工シナリオによって表現することができる。このことは分散オブジェクトシステムについても同様であり、分散オブジェクトシステム上に存在するデータベースのデータコンテンツを利用して加工データコンテンツを作成した場合にも、利用したデータベース，利用した原データコンテンツ，使用した加工ツールの情報及び加工シナリオを特定することによって加工データコンテン

ツを再現することができ、このことは単一のデータベースあるいは複数のデータベースから入手した複数のデータコンテンツを利用した場合であっても同様である。

【００７８】図５により実施例４を説明する。この実施例において、データコンテンツを保有している原著作権者及び情報提供業者（ＩＰ）はデータコンテンツを保有していないユーザと区別されてデータ管理センタ等とともにネットワーク側に配置される。この実施例のシステムにおいては公開鍵及び専用鍵が使用される。なお、原データコンテンツがユーザに転送されるときには、安全のために原データコンテンツは秘密鍵をあるいは転送先の公開鍵を用いて暗号化される。

【００７９】第１ユーザU1はネットワーク，放送あるいは記録媒体を利用して、データコンテンツの探索を行い必要なデータコンテンツを収集するが、収集された著作物データはユーザU1のメモリ上に１時的に保存されるに止まり、ハードディスクドライブ（HDD）等のデータ保存装置がユーザU1の装置に含まれている場合でもデータコンテンツがデータ保存装置に保存されることはない。データコンテンツが保存されることがないようにするために、保存が行われようとした場合に、メモリ上の著作物データの破壊、メモリ上のデータヘッダの変更、データコンテンツの一方向ハッシュ値化、ファイル名の保存不能ファイル名への変更等が行われることによりデータコンテンツの保存禁止が行われる。保存禁止は、オブジェクト構造を有するデータコンテンツのプログラム部分に内蔵されたデータ保存禁止プログラムによって行うこともできるが、システム全体あるいはユーザの装置に関わるオペレーティングシステム（ＯＳ）によって行われることにより高度の信頼性が得られる。

【００８０】複数のデータコンテンツを利用する場合について説明する。

(1),(2) 第１ユーザU1は第１ユーザラベルLu1を、データ管理センタに提示して、システム内の情報提供者ＩＰのデータライブラリから原データM0i（i=1,2,3...）を収集し、加工ツールPeを入手するが、このとき原データコンテンツM0i及び加工ツールPeは第１ユーザU1の公開鍵Kb1を用いて暗号化されて、

Cm0ikb1＝E（M0i，Kb1）

Cpekb1＝E（Pe，Kb1）

暗号化原データコンテンツCm0ikb1及び暗号化加工ツールCpekb1が、第１ユーザU1に配付される。なお、このとき第１ユーザラベルLu1が参照されることにより、原データコンテンツM0i及び加工ツールPeの利用状況もデータ管理センタに記録され、課金に利用される。

【００８１】(3) 暗号化原データコンテンツCm0ikb1及び暗号化加工ツールCpekb1を配布された第１ユーザU1は、配布された暗号化原データコンテンツCm0ikb1及び暗号化加工ツールCpekb1を第１ユーザU1の専用鍵Kv1を用いて復号し、

M0i＝D（Cm0ikb1，Kv1）

Pe＝D（Cpekb1，Kv1）

し、復号された加工ツールPeを使用して復号された原データコンテンツM0iを加工し、第１加工データコンテンツM1i(i=1,2,3...)を得る。

【００８２】(4) 第１加工データコンテンツM1iを得た第１ユーザU1は、第１加工著作物データコンテンツM1iについての加工データである第１シナリオS1iをデータ管理センタの公開鍵Kbcで暗号化し、

Cslikbc＝E（S1i，Kbc）

暗号化第１シナリオCslikbcを第１ユーザラベルLu1とともに、データ管理センタに提示し、このことによってユーザU1の二次著作権の登録が行われる。

【００８３】(5) 暗号化第１シナリオCslikbcを提示されたデータ管理センタは、暗号化第１シナリオCslikbcをデータ管理センタの専用鍵Kvcを用いて復号し、

S1i＝D（Cslikbc，Kvc）

提示された第１ユーザU1のユーザラベルと復号された第１シナリオS1iに基づき第１加工ラベルLe1を作成し、データ管理センタ内に保管し、第１加工ラベルLe1を第１ユーザU1の公開鍵Kb1を用いて暗号化し、

Cle1kb1＝E（Le1，Kb1）

暗号化第１加工ラベルCle1kb1を、第１ユーザU1に転送する。

【００８４】(6) 暗号化第１加工ラベルCle1kb1を転送された第１ユーザU1は、暗号化第１加工ラベルCle1kb1を第１ユーザU1の専用鍵Kv1を用いて復号し、

Le1＝D（Cle1kb1，Kv1）

復号された第１加工ラベルLe1を第２ユーザU2の公開鍵Kb2を用いて暗号化し、

Cle1kb2＝E（Le1，Kb2）

暗号化第１加工ラベルCle1kb2を、第２ユーザU2に転送するが、第１加工著作物データコンテンツM1iあるいは暗号化第１加工著作物データが第２ユーザU2に転送されることはない。

【００８５】第１ユーザU1のコンピュータがデータ保存装置を有しているときには収集データコンテンツあるいは加工データコンテンツがデータ保存装置に保存される可能性があるが、保存・複写及び転送を阻止するために、上述の保存禁止が行われる。なお、この場合暗号化第１加工ラベルCle1kb2の代わりに、第１加工ラベルを一方向ハッシュ値化した電子指紋F1を使用することもでき、このようにすることにより電話音声による簡略化された加工ラベルの転送が可能になる。

【００８６】(7) 暗号化第１加工ラベルCle1kb2を転送された第２ユーザU2は、転送された暗号化第１加工ラベルCle1kb2を第２ユーザU2の専用鍵Kv2を用いて復号し、

Le1＝D（Cle1kb2，Kv2）

第１加工ラベルLe1を第２ユーザU2の専用鍵Kv2を用

いて暗号化し、
Ｃｌｅｌｋｖ２＝Ｅ（Ｌｅｌ，Ｋｖ２）
暗号化第１加工ラベルＣｌｅｌｋｖ２を第２ユーザラベルＬｕ２とともに、データ管理センタに提示する。
【００８７】(8) 暗号化第１加工ラベルＣｌｅｌｋｖ２と第２ユーザラベルＬｕ２を提示されたデータ管理センタは、提示された暗号化第１加工ラベルＣｌｅｌｋｖ２を第２ユーザＵ２の公開鍵Ｋｂ２を用いて復号し、
Ｌｅｌ＝Ｄ（Ｃｌｅｌｋｖ２，Ｋｂ２）
復号された第１加工ラベルＬｅｌに記載された原データコンテンツＭ０ｉを収集し、原データＭ０ｉを加工ツールＰｅを用いて同じく第１加工ラベルＬｅｌに記載された第１シナリオＳ１ｉに基づいて加工して第１加工データコンテンツＭ１ｉを再生する。
【００８８】第１加工データコンテンツＭ１ｉを再生したデータ管理センタは、第１加工データコンテンツＭ１ｉ及び加工ツールＰｅを第２ユーザＵ２の公開鍵Ｋｂ２を用いて暗号化し、
Ｃｍｌｉｋｂ２＝Ｅ（Ｍ１ｉ，Ｋｂ２）
Ｃｐｅｋｂ２＝Ｅ（Ｐｅ，Ｋｂ２）
暗号化第１加工データコンテンツＣｍｌｉｋｂ２及び暗号化加工ツールＣｐｅｋｂ２を、第２ユーザＵ２に転送する。
【００８９】(9) 暗号化第１加工データコンテンツＣｍｌｉｋｂ２び暗号化加工ツールＣｐｅｋｂ２を配布された第２ユーザＵ２は、配布された暗号化第１データコンテンツＣｍｌｉｋｂ２及び暗号化加工ツールＣｐｅｋｂ２を第２ユーザＵ２の専用鍵Ｋｖ２を用いて復号し、
Ｍ１ｉ＝Ｄ（Ｃｍｌｉｋｂ２，Ｋｖ２）
Ｐｅ＝Ｄ（Ｃｐｅｋｂ２，Ｋｖ２）
し、復号された加工ツールＰｅを使用して復号された第１加工データコンテンツＭ１ｉを加工し、第２加工データコンテンツＭ２ｉ(i=1, 2, 3...)を得る。
【００９０】(10) 第２加工著作物データコンテンツＭ２ｉを得た第２ユーザＵ２は、第２加工データコンテンツＭ２ｉについての加工データである第２シナリオＳ２ｉをデータ管理センタの公開鍵Ｋｂｃで暗号化し、
Ｃｓ２ｉｋｂｃ＝Ｅ（Ｓ２ｉ，Ｋｂｃ）
暗号化第２シナリオＣｓ２ｉｋｂｃを第２ユーザラベルＬｕ２とともに、データ管理センタに提示する。
【００９１】(11) 暗号化第２シナリオＣｓ２ｉｋｂｃを提示されたデータ管理センタは、暗号化第２シナリオＣｓ２ｉｋｂｃをデータ管理センタの専用鍵Ｋｖｃを用いて復号し、
Ｓ２ｉ＝Ｄ（Ｃｓ２ｉｋｂｃ，Ｋｖｃ）
提示された第２ユーザＵ２のユーザラベルと復号された第２シナリオＳ２ｉに基づき第２加工ラベルＬｅ２を作成し、データ管理センタ内に保管し、第２加工ラベルＬｅ２を第１ユーザＵ２の公開鍵Ｋｂ２を用いて暗号化し、
Ｃｌｅ２ｋｂ２＝Ｅ（Ｌｅ２，Ｋｂ２）
暗号化第２加工ラベルＣｌｅ２ｋｂ２を、第２ユーザＵ２に転送する。
【００９２】(12) 暗号化第２加工ラベルＣｌｅ２ｋｂ２を転送された第２ユーザＵ２は、暗号化第２加工ラベルＣｌｅ２ｋｂ２を第２ユーザＵ２の専用鍵Ｋｖ２を用いて復号し、
Ｌｅ２＝Ｄ（Ｃｌｅ２ｋｂ２，Ｋｖ２）
復号された第２加工ラベルＬｅ２を第３ユーザＵ３の公開鍵Ｋｂ３を用いて暗号化し、
Ｃｌｅ２ｋｂ３＝Ｅ（Ｌｅ２，Ｋｂ３）
暗号化第２加工ラベルＣｌｅ２ｋｂ３を、第３ユーザＵ３に転送する。以後、同様な動作が繰り返される。
【００９３】この分散オブジェクトシステムを利用する実施例４では、データコンテンツはユーザが保存せず、データベースにのみ保存されている、一方ユーザはユーザの情報及び加工に関する情報すなわち、利用した原データコンテンツ，使用した加工ツールの情報及び加工シナリオ及び加工したユーザ情報が記載された加工ラベルのみを管理保存し、この加工ラベルのみが暗号化されてユーザ間で転送される。したがって、著作物データコンテンツが保存・複写あるいは転送されることはない。
【００９４】なお、再暗号用の鍵が復号用の鍵と同時に配布されるシステムと、再暗号用の鍵が復号用の鍵と別々に配布されるシステムとを一つのシステム中に共存させ、適宜選択して利用するように構成することも可能である。
【００９５】［実施例５］原データコンテンツ及び加工データコンテンツを流通させるデータコンテンツ流通システムの実施例を図６により説明する。このシステムにおいて取り扱われる原データコンテンツはオブジェクトであり、加工データコンテンツは原データコンテンツオブジェクトを加工シナリオによってリンクさせたものとして表現される。したがって、流通するのは加工シナリオのみであり、加工シナリオを入手したユーザは加工シナリオに従って使用されている原データコンテンツを収集しリンクさせて加工データコンテンツを再現させる。この場合、原データコンテンツの収集及びリンク作業はユーザ自身が行ってもよいが、システム側で行うかあるいはエージェントプログラムに行わせれば負担が軽減される。
【００９６】このシステムの中核をなすデータコンテンツ流通センタは、ネットワーク上に存在するデータコンテンツデータベース，加工シナリオデータベース，鍵管理センタ，データコンテンツ流通管理センタから構成されている。データコンテンツデータベースは、情報提供者（ＩＰ）が供給した原データコンテンツを保存し、ユーザの要求に対応して供給する。シナリオデータベースは、ユーザが原データコンテンツあるいはユーザが創作したユーザデータコンテンツを利用して加工データコンテンツを得た場合の加工シナリオを保存し、ユーザの要求に対応して供給する。鍵管理センタは、原データコンテンツ，ユーザデータコンテンツ及び加工シナリオの暗号／復号用秘密鍵を保存し、ユーザの要求に対応して供

給する。データコンテンツ流通管理センタは、原データコンテンツあるいは加工データコンテンツをカタログ化して広告し、ユーザへの販売管理及び課金を行うとともにデータコンテンツデータベースに保存されるデータコンテンツの著作権ラベルの管理を行う。加工シナリオ流通管理センタは、加工データコンテンツをカタログ化して広告し、ユーザへの販売管理及び課金を行う。さらに、必要に応じて加工シナリオに基づいて原データコンテンツの収集及びリンク作業を行うとともに加工シナリオデータベースに保存される加工シナリオの加工ラベルの管理を行う。これらデータコンテンツ流通センタを構成する各要素の具体的な動作については、これまでに説明した内容と重複するため、ここでは説明を省略する。

【００９７】(1) 情報提供者ＩＰi（i=1, 2, 3...、以降同様）は、原データコンテンツM0iを原秘密鍵Ks0iを用いて暗号化し、

Cm0iks0i＝E（M0i, Ks0i）

対応する原秘密鍵Ks0iをデータコンテンツ流通センタの公開鍵Kbcを用いて暗号化し、

Cks0ikbc＝E（Ks0i, Kbc）

暗号化原データコンテンツCm0iks0i（図では"m0i"と表示）及び暗号化原秘密鍵Cks0ikbc（図では"ks0i"と表示）をデータコンテンツ流通センタに供給する。

【００９８】原秘密鍵Ks0iは情報提供者ＩＰiが用意してもあるいは情報提供者ＩＰiが鍵管理センタに生成を依頼してもよい。原秘密鍵Ks0iを鍵管理センタが生成する場合には生成された原秘密鍵Ks0iは情報提供者ＩＰiの公開鍵Kb0iを用いて暗号化されて、

Cks0ikb0i＝E（Ks0i, Kv0i）

暗号化原秘密鍵Cks0ikb0iが情報提供者ＩＰiに配送され、情報提供者ＩＰiは専用鍵Kv0iを用いて復号し、

Ks0i＝D（Cks0ikb0i, Kb0i）

復号された原秘密鍵Ks0iを原データコンテンツM0iの暗号化に用いる。

【００９９】データコンテンツ流通センタは、供給された暗号化原秘密鍵Cks0ikbcをデータコンテンツ流通センタの専用鍵Kvcを用いて復号化し、

Ks0i＝D（Cks0ikbc, Kvc）

復号された原秘密鍵Ks0iを用いて暗号化原データコンテンツCm0iks0iを復号し、

M0i＝D（Cm0iks0i, Ks0i）

復号された原データコンテンツM0i及びこれに対応する原秘密鍵Ks0iをデータコンテンツデータベースに保存する。なお、情報提供者あるいはデータコンテンツ流通センタが原データコンテンツM0iに不正利用確認のための透かしを付与して保存することもできる。

【０１００】コンテンツ流通管理センタは原データコンテンツの利用促進のため、原データコンテンツをそのままでは利用することができないように縮小あるいは部分化する等の手段によりカタログ化してデータコンテンツ流通センタ内に掲示する。

【０１０１】(2) カタログ化された原データコンテンツを閲覧した第１ユーザU1iは、第１ユーザラベルLu1i及び第１ユーザU1iの公開鍵Kb1iを提示し、利用を希望する原データコンテンツを指定してデータコンテンツ流通センタに利用申込みを行う。

【０１０２】(3) 原データコンテンツM0iの利用申込みを受けたデータコンテンツ流通センタは、課金及び身元確認のためユーザラベルLu1iを確認し、原データコンテンツM0iを対応する原秘密鍵Ks0iを用いて暗号化し、

Cm0iks0i＝E（M0i, Ks0i）

原秘密鍵Ks0iを第１ユーザU1iの公開鍵Kb1iを用いて暗号化し、

Cks0ikb1i＝E（Ks0i, Kb1i）

暗号化原データコンテンツCm0iks0i及び暗号化原秘密鍵Cks0ikb1i（図では"ks0i"と表示）を第１ユーザU1iに配送するとともに、原データコンテンツの使用について第１ユーザU1iに対する課金を行う。

【０１０３】(4) 暗号化原データコンテンツCm0iks0i及び暗号化原秘密鍵Cks0ikb1iを配送された第１ユーザU1iは、暗号化原秘密鍵Cks0ikb1iを第１ユーザU1iの専用鍵Kv1iを用いて復号し、

Ks0i＝D（Cks0ikb1i, Kv1i）

次に復号された原秘密鍵Ks0iを用いて暗号化原データコンテンツCm0iks0iを復号し、

M0i＝D（Cm0iks0i, Ks0i）

復号された原データコンテンツM0iを利用して新規な第１加工データコンテンツM1iを作成する。

【０１０４】前に述べたように、データコンテンツの加工には単一の原データコンテンツを利用する場合と、複数の原データコンテンツを利用する場合があり、これらにはさらにユーザのデータコンテンツが加えられる場合がある。したがって、この実施例において加工に利用されるデータコンテンツには単一のデータコンテンツの他に、複数の原データコンテンツ、ユーザのデータコンテンツがあり、これらのデータコンテンツと加工内容である加工シナリオによって加工データコンテンツは構成され、すなわちこれらを入手することにより加工データコンテンツを再現することができる。

【０１０５】ところで、原データコンテンツは本来データコンテンツ流通センタのデータコンテンツデータベースに保存されているものであるから、データコンテンツの加工によって新規に生成されたことによりデータコンテンツ流通センタに未だ保存されていないデータはユーザのデータコンテンツと加工シナリオである。したがって、これらをデータコンテンツ流通センタに保存することによりデータコンテンツの加工を行ったユーザの第１ユーザデータコンテンツを原データコンテンツと同様に取り扱うことが可能になり、そのユーザも情報提供者と

なることが可能になる。

【０１０６】(5) 第１加工データコンテンツM1iは、原データコンテンツM0iと第１加工シナリオS1iから構成され、さらに場合によっては構成要素として第１ユーザデータコンテンツMuliが加えられる。これらの要素中、原データコンテンツM0iはデータコンテンツ流通センタのデータコンテンツデータベースに保存されているから、新規にデータコンテンツ流通センタに保存する必要があるのは第１加工シナリオS1iと第１ユーザデータコンテンツMuliである。

【０１０７】そのために第１ユーザU1iは第１秘密鍵Ksliを用意し、第１加工シナリオS1iと第１ユーザデータコンテンツMuliを第１秘密鍵Ksliを用いて暗号化し、

Csliksli＝E（S1i，Ksli）

Cmuliksli＝E（Muli，Ksli）

第１秘密鍵Ksliをデータコンテンツ流通センタの公開鍵Kbcを用いて暗号化し、

Ckslikbc＝E（Ksli，Kbc）

暗号化第１加工シナリオCsliksli（図では、"s1i"と表示），暗号化第１ユーザデータコンテンツCmuliksli（図では、"m1i"と表示）及び暗号化第１秘密鍵Cksli kbc（図では、"ksli"と表示）をデータコンテンツ流通センタに転送する。

【０１０８】第１秘密鍵Ksliは第１ユーザU1iが用意してもあるいは第１ユーザU1iが鍵管理センタに生成を依頼してもよい。第１秘密鍵Ksliを鍵管理センタが生成する場合には生成された第１秘密鍵Ksliは第１ユーザU1iの公開鍵Kbliを用いて暗号化されて、

Ckslikbli＝E（Ksli，Kbli）

暗号化第１秘密鍵Cklikbliが第１ユーザU1iに配送され、第１ユーザU1iは専用鍵Kvliを用いて復号し、

Ksli＝D（Ckslikbli，Kvli）

復号された第１秘密鍵K1iを第１加工シナリオS1i及び第１ユーザデータコンテンツMuliの暗号化に用いる。

【０１０９】データコンテンツ流通センタは、データコンテンツ流通センタの専用鍵Kvcを用いて転送された暗号化第１秘密鍵Ckslikbcを復号し、

Ksli＝D（Ckslikbc，Kvc）

復号された第１秘密鍵Ksliを用いて暗号化第１加工シナリオCsliksli及び暗号化第１ユーザデータコンテンツCuliksliを復号し、

S1i＝D（Csliksli，Ksli）

Muli＝D（Cmuliksli，Ksli）

第１ユーザラベルに基づいて第１ユーザデータコンテンツラベル及び第１加工シナリオラベルを生成し、復号された第１秘密鍵Ksli，第１加工シナリオS1i，第１ユーザデータコンテンツMuli及び第１ユーザデータコンテンツラベル及び第１加工シナリオラベルををデータベースに保存する。なお、第１ユーザあるいはデータコンテンツ流通センタが原データコンテンツM0iに不正利用確認のための透かしを付与して保存することもできる。第１秘密鍵Ksli，第１加工シナリオS1i及び第１ユーザデータコンテンツMuliを保存するデータベースは原データコンテンツM0iが保存されているデータコンテンツデータベースであっても、また別にシナリオデータベースを設けることも可能である。

【０１１０】コンテンツ流通管理センタは第１加工データコンテンツの利用促進のため、第１加工データコンテンツをそのままでは利用することができないように縮小あるいは部分化する等の手段によりカタログ化してデータコンテンツ流通センタ内に掲示する。

【０１１１】(6) カタログ化された原データコンテンツM0i及び第１加工データコンテンツM1iを閲覧した第２ユーザU2iは、第２ユーザラベルLu2i及び第２ユーザU2iの公開鍵Kb2iを提示し、利用を希望する原データコンテンツM0i及び／又は第１加工データコンテンツM1iを指定してデータコンテンツ流通センタに利用申込みを行う。

【０１１２】(7) 原データコンテンツM0i及び／又は第１加工データコンテンツM1iの利用申込みを受けたデータコンテンツ流通センタは、課金及び身元確認のためユーザラベルLu2iを確認し、利用申込みが行われた原データコンテンツM0iを対応する原秘密鍵Ks0iを用いて、第１加工シナリオS1i及び第１ユーザデータコンテンツMuliを第１秘密鍵Ksliを用いて、原秘密鍵Ks0iを公開鍵Kb2iを用いて、第１秘密鍵Ksliを公開鍵Kb2iを用いて、各々暗号化し、

Cm0iks0i＝E（M0i，Ks0i）

Csliksli＝E（S1i，Ksli）

Cmuliksli＝E（Muli，Ksli）

Cks0ikb2i＝E（Ks0i，Kb2i）

Ckslikb2i＝E（Ksli，Kb2i）

暗号化原データコンテンツCm0iks0i（図では"m0i"と表示），暗号化第１加工シナリオCsliksli（図では"s1i"と表示），暗号化第１ユーザデータコンテンツCmuliksli（図では"muli"と表示），暗号化原秘密鍵Cks0ikb2i及び暗号化第１秘密鍵Ckslikb2iを第２ユーザU2iに転送するとともに、原データコンテンツM0i及び第１加工シナリオS1iの使用について第２ユーザU2iに対する課金を行う。

【０１１３】(8) 暗号化原データコンテンツCm0iks0i，暗号化第１加工シナリオCsliksli，暗号化第１ユーザデータコンテンツCmuliksli，暗号化原秘密鍵Cks0ikb2i及び暗号化第１秘密鍵Ckslikb2iを転送された第２ユーザU2iは暗号化原秘密鍵Cks0ikb2i及び暗号化第１秘密鍵Ckslikb2iを第２ユーザU2iの専用鍵Kv2iを用いて復号し、

Ks0i＝D（Cks0ikb2i，Kv2i）

Ksli＝D（Ckslikb2i，Kv2i）

次に復号された原秘密鍵Ks0iを用いて暗号化原データコンテンツCm0iks0iを、復号された第１秘密鍵Ksliを用いて暗号化第１加工シナリオCsliksli及び暗号化第１ユーザデータコンテンツCmuliksliを復号し、
M0i＝D（Cm0iks0i，Ks0i）
Sli＝D（Csliksli，Ksli）
Muli＝D（Cmuliksli，Ksli）
復号された原データコンテンツM0i，第１加工シナリオSli及び第１ユーザデータコンテンツMuliを利用して新規な第２加工データコンテンツM2iを作成する。

【０１１４】第２ユーザU2iは第２秘密鍵Ks2iを用意し、データコンテンツ流通センタのデータベースに保存されていない新規なデータである第２加工シナリオS2iと第２ユーザデータコンテンツMu2iを第２秘密鍵Ks2iを用いて暗号化し、
Cs2iks2i＝E（S2i，Ks2i）
Cmu2iks2i＝E（Mu2i，Ks2i）
第２秘密鍵Ks2iをデータコンテンツ流通センタの公開鍵Kbcを用いて暗号化し、
Cks2ikbc＝E（Ks2i，Kbc）
暗号化第２加工シナリオCs2iks2i（図では"s2i"と表示），暗号化第２ユーザデータコンテンツCmu2iks2i（図では"mu2i"と表示）及び暗号化第２秘密鍵Cks2ikbc（図では"ks2i"と表示）をデータコンテンツ流通センタに転送する。以後、同様な動作が繰り返される。

【０１１５】［実施例６］データコンテンツ加工者が加工シナリオの使用権をデータコンテンツ取引市場において競売で販売する実施例を図７により説明する。この実施例において加工シナリオの使用権はシステム上の取引市場において競売され、加工シナリオの使用権を入手した加工シナリオ販売者は加工シナリオをユーザに販売あるいは貸与する。

【０１１６】このシステムにおいて取り扱われる原データコンテンツはオブジェクトであり、加工データコンテンツは原データコンテンツオブジェクトを加工シナリオによってリンクさせたものとして表現される。したがって、売買されるのは加工シナリオのみであり、加工シナリオを購入あるいは借用したユーザは加工シナリオに従って使用されている原データコンテンツを収集しリンクさせて加工データコンテンツを再現させる。この場合、原データコンテンツの収集はユーザ自身が行ってもよいが、システム側で行うかあるいはエージェントプログラムに行わせれば負担が軽減される。

【０１１７】このシステムの中核をなすデータコンテンツ流通センタは、ネットワーク上に存在する鍵管理センタ，データコンテンツデータベース，データコンテンツ流通管理センタ，加工シナリオデータベース，加工シナリオ競売管理センタから構成されている。データコンテンツデータベースは、情報提供者が供給した原データコンテンツを保存し、データコンテンツ加工者に供給する。加工シナリオデータベースは、データコンテンツ加工者が原データコンテンツあるいはデータコンテンツ加工者が創作した加工者データコンテンツを利用して加工データコンテンツを得た場合の加工シナリオを保存し、競売に参加する加工シナリオ販売者に供給する。鍵管理センタは、原データコンテンツ，加工者データコンテンツ及び加工シナリオの暗号／復号用秘密鍵を保存し、データコンテンツ加工者あるいは加工シナリオ販売者に供給する。データコンテンツ流通管理センタは、原データコンテンツをカタログ化して広告し、データコンテンツ加工者への販売管理を行う。加工シナリオ競売管理センタは、加工データコンテンツをカタログ化して広告し、加工シナリオ競売の管理及び課金を行う。さらに、必要に応じて加工シナリオに基づいて原データコンテンツの収集及びリンク作業を行うとともに加工シナリオデータベースに保存される加工シナリオの加工ラベルの管理を行う。これらデータコンテンツ流通センタを構成する各要素の具体的な動作については、これまでに説明した内容と重複するため、ここでは説明を省略する。

【０１１８】(1) 情報提供者ＩＰi（i=1,2,3...、以降同様）は、原データコンテンツM0iを原秘密鍵K0iを用いて暗号化し、
Cm0iks0i＝E（M0i，Ks0i）
対応する原秘密鍵Ks0iをデータコンテンツ流通センタの組織公開鍵Kbcを用いて暗号化し、
Cks0ikbc＝E（Ks0i，Kbc）
暗号化原データコンテンツCm0iks0i（図では"m0i"と表示）及び暗号化原秘密鍵Cks0ikbc（図では"ks0i"と表示）をデータコンテンツ流通センタに供給する。

【０１１９】原秘密鍵Ks0iは情報提供者ＩＰiが用意してもあるいは情報提供者ＩＰiが鍵管理センタに生成を依頼してもよい。原秘密鍵Ks0iを鍵管理センタが生成する場合には生成された原秘密鍵Ks0iは情報提供者ＩＰiの公開鍵Kb0iを用いて暗号化されて、
Cks0ikb0i＝E（Ks0i，Kv0i）
暗号化原秘密鍵Cks0ikb0iが情報提供者ＩＰiに配送され、情報提供者ＩＰiはＩＰ専用鍵Kv0iを用いて復号し、
Ks0i＝D（Cks0ikb0i，Kb0i）
復号された原秘密鍵Ks0iを原データコンテンツM0iの暗号化に用いる。

【０１２０】データコンテンツ流通センタは、供給された暗号化原秘密鍵Cks0ikbcをデータコンテンツ流通センタの専用鍵Kvcを用いて復号し、
Ks0i＝D（Cks0ikbc，Kvc）
復号された原秘密鍵Ks0iを用いて暗号化原データコンテンツCm0iks0iを復号し、
M0i＝D（Cm0iks0i，Ks0i）
復号された原データコンテンツM0i及びこれに対応する原秘密鍵Ks0iをデータコンテンツデータベースに保存

する。なお、情報提供者あるいはデータコンテンツ流通センタが原データコンテンツM0iに不正利用確認のための透かしを付与して保存することもできる。

【０１２１】コンテンツ流通管理センタは原データコンテンツの加工利用促進のため、原データコンテンツをそのままでは利用することができないように縮小あるいは部分化する等の手段によりカタログ化してデータコンテンツ流通センタ内に掲示する。

【０１２２】(2) カタログ化された原データコンテンツを閲覧したデータコンテンツ加工者Eiは、データコンテンツ加工者ラベルLei及びデータコンテンツ加工者Eiの公開鍵Kbliを提示し、利用を希望する原データコンテンツを指定してデータコンテンツ流通センタに利用申込みを行う。

【０１２３】(3) 原データコンテンツM0iの利用申込みを受けたデータコンテンツ流通センタは、課金及び身元確認のためユーザラベルLeiを確認し、原データコンテンツM0iを対応する原秘密鍵Ks0iを用いて暗号化し、

Cm0iks0i＝E（M0i，Ks0i）

原秘密鍵Ks0iをデータコンテンツ加工者Eiの公開鍵Kbeiを用いて暗号化し、

Cks0ikbei＝E（Ks0i，Kbei）

暗号化原データコンテンツCm0iks0i及び暗号化原秘密鍵Cks0ikbei（図では"ks0i"と表示）をデータコンテンツ加工者Eiに配送するとともに、原データコンテンツの使用についてデータコンテンツ加工者Ei及び最終ユーザに対する課金を行う。

【０１２４】(4) 暗号化原データコンテンツCm0iks0i及び暗号化原秘密鍵Cks0ikbeiを配送されたデータコンテンツ加工者Eiは、暗号化原秘密鍵Cks0ikbeiをデータコンテンツ加工者Eiの専用鍵Kveiを用いて復号し、

Ks0i＝D（Cks0ikbei，Kvei）

次に復号された原秘密鍵Ks0iを用いて暗号化原データコンテンツCm0iks0iを復号し、

M0i＝D（Cm0iks0i，Ks0i）

復号された原データコンテンツM0iを利用して加工データコンテンツMeiを作成する。

【０１２５】前に述べたように、データコンテンツの加工には単一の原データコンテンツを利用する場合と、複数の原データコンテンツを利用する場合があり、これらにはさらにデータコンテンツ加工者のデータコンテンツが加えられる場合がある。したがって、この実施例において加工に利用されるデータコンテンツには単一のデータコンテンツの他に、複数の原データコンテンツ、データコンテンツ加工者のデータコンテンツがあり、これらのデータコンテンツと加工内容である加工シナリオによって加工データコンテンツは構成され、すなわちこれらを入手することにより加工データコンテンツを再現することができる。

【０１２６】ところで、原データコンテンツは本来データコンテンツ流通センタのデータコンテンツデータベースに保存されているものであるから、データコンテンツの加工によって新規に生成されたことによりデータコンテンツ流通センタに未だ保存されていないデータはデータコンテンツ加工者の加工者データコンテンツと加工シナリオである。したがって、これらをデータコンテンツ流通センタに保存することによりデータコンテンツの加工を行ったデータコンテンツ加工者の加工者データコンテンツを原データコンテンツと同様に取り扱うことが可能になり、そのデータコンテンツ加工者も情報提供者となることが可能になりる。そして、さらには加工シナリオ及び／又は加工者データコンテンツの使用権を市場で競売によって売却することも可能である。なお、加工シナリオ及び加工者データコンテンツの使用権の数は１個の加工データコンテンツについて複数個とすることが可能である。

【０１２７】(5) 加工データコンテンツMeiは、原データコンテンツM0iと加工シナリオSeiから構成され、さらに場合によっては構成要素として加工者データコンテンツMeiが加えられている。これらの要素中、原データコンテンツM0iはデータコンテンツ流通センタのデータコンテンツデータベースに保存されているから、データコンテンツ加工者の新規にデータコンテンツ流通センタに保存する必要があるのは加工シナリオS1iと加工者データコンテンツMediである。

【０１２８】加工シナリオS1i及び加工者データコンテンツMediの使用権を売却するために、データコンテンツ加工者Eiは秘密鍵Kseiを用意し、加工シナリオSeiと加工者データコンテンツMediを秘密鍵Kseiを用いて暗号化し、

Cseiksei＝E（Sei，Ksei）

Cmediksei＝E（Medi，Ksei）

秘密鍵Kseiをデータコンテンツ流通センタの公開鍵Kbcを用いて暗号化し、

Ckseikbc＝E（Ksei，Kbc）

暗号化加工シナリオCseiksei（図では、"sei"と表示），暗号化加工者データコンテンツCmediksei（図では"medi"と表示）及び暗号化秘密鍵Ckseikbc（図では、"ksei"と表示）をデータコンテンツ流通センタに転送する。

【０１２９】秘密鍵Kseiはデータコンテンツ加工者Eiが用意してもあるいはデータコンテンツ加工者Eiが鍵管理センタに生成を依頼してもよい。秘密鍵Kseiを鍵管理センタが生成する場合には生成された秘密鍵Kseiはデータコンテンツ加工者Eiの公開鍵Kbeiを用いて暗号化されて、

Ckseikbei＝E（Ksei，Kbei）

暗号化秘密鍵Ckeikbeiがデータコンテンツ加工者Eiに配送され、データコンテンツ加工者Eiは専用鍵Kveiを用いて復号し、

Ｋsei＝Ｄ（Ckseikbei，Kvei）
復号された秘密鍵Keiを加工シナリオＳei及びデータコンテンツ加工者データコンテンツMediの暗号化に用いる。

【０１３０】データコンテンツ流通センタは、データコンテンツ流通センタの専用鍵Kvcを用いて転送された暗号化秘密鍵Ckseikbcを復号し、
Ｋsei＝Ｄ（Ckseikbc，Kvc）
復号された秘密鍵Kseiを用いて暗号化加工シナリオＣseiksei及び暗号化加工者データコンテンツＣmedikseiを復号し、
Ｓei＝Ｄ（Cseiksei，Ksei）
Medi＝Ｄ（Cmediksei，Ksei）
復号された秘密鍵Ksei，加工シナリオＳei及び加工者データコンテンツMediに各々データコンテンツ加工者ラベルＬeiに基づく著作権ラベルを付けてデータベースに保存する。なお、データコンテンツ加工者あるいはデータコンテンツ流通センタが加工シナリオＳei及び加工者データコンテンツMediに不正利用確認のための透かしを付与して保存することもできる。秘密鍵Ksei，加工シナリオＳei及びデータコンテンツ加工者データコンテンツMediを保存するデータベースは原データコンテンツM0iが保存されているデータコンテンツデータベースであっても、また別にシナリオデータベースを設けることも可能である。

【０１３１】データコンテンツ流通センタ内のシナリオ市場管理センタは加工シナリオ及び加工者データコンテンツの競売を行うために、加工データコンテンツをそのままでは利用することができないように縮小あるいは部分化する等の手段によりカタログ化し、販売する使用権の数を示してシナリオ販売管理センタ内に掲示して、競売を行うことを告示する。

【０１３２】(6) カタログ化された加工データコンテンツMeiを閲覧した複数の加工シナリオ販売者Ｄiは、加工シナリオ販売者ラベルＬdi及び加工シナリオ販売者Ｄiの公開鍵Kbdiを提示して加工シナリオＳei及びデータコンテンツ加工者データコンテンツMediの購入申込みを加工シナリオ市場管理センタに行う。

【０１３３】(7) 加工シナリオＳei及びデータコンテンツ加工者データコンテンツMediの購入申込みを受けた加工シナリオ市場管理センタは、課金及び身元確認のため加工シナリオ販売者ラベルＬdiを確認し、ネットワーク上で競売を行い複数の加工シナリオ販売者Ｄiに加工シナリオＳei及びデータコンテンツ加工者データコンテンツMediの使用権を売却する。なお、前に述べたように加工シナリオ及び加工者データコンテンツの使用権の数は１個の加工データコンテンツについて複数個とすることが可能である。売却先に決定した加工シナリオ販売者Ｄiは、加工シナリオ販売者Ｄiの秘密鍵Ksdiをデータコンテンツ流通センタの公開鍵Kbcを用いて暗号化して、

Cksdikbc＝Ｅ（Ksdi，Kbc）
暗号化秘密鍵Cksdikbc（図では、"ksdi"と表示）を加工シナリオ市場管理センタに配送する。

【０１３４】(8) 加工シナリオ市場管理センタは提示された暗号化秘密鍵Cksdikbcをデータコンテンツ流通センタの専用鍵Kvcを用いて復号し、
Ｋsdi＝Ｄ（Cksdikbc，Kvc）
復号された加工シナリオ販売者Ｄiの秘密鍵Ksdiを用いて加工シナリオＳei及びデータコンテンツ加工者データコンテンツMediを暗号化し、
Ｃseiksdi＝Ｅ（Sei，Ksdi）
Ｃmediksdi＝Ｅ（Medi，Ksdi）
暗号化加工シナリオＣseiksdi及び暗号化データコンテンツ加工者データコンテンツＣmediksdiを加工シナリオ販売者Ｄiに送付する。また、著作権ラベルの内容はデータコンテンツ加工者ラベルＬeiに基づくものからシナリオ販売者ラベルＬdiに基づくものに変更され、その結果、データコンテンツ加工者の秘密鍵Kseiは使用不可能となり、代わって加工シナリオ販売者の秘密鍵Ksdiが使用可能となる。なお、この場合著作権ラベルの内容を変更することなく、新規に加工シナリオ販売者ラベルＬdiに基づくものを追加することもできる。

【０１３５】暗号化加工シナリオＣseiksdiを購入した加工シナリオ販売者は以後において、購入した加工シナリオの使用権を行使する。なお、原データコンテンツも加工シナリオと同様に競売によって販売することが可能であるが、原データコンテンツの利用者は複数となることもあり得るため、特定の販売者に売却することは避けた方がよい。以後、必要ならば同様な動作が繰り返される。

【０１３６】本明細書に示された各実施例のデータコンテンツ流通システムにおいて、ユーザ側装置としてハードディスクドライブ等の保存装置を有しないネットワークコンピュータが使用される場合にはデータコンテンツの無料使用，流出等の不正使用問題は生じにくいが、ユーザ側装置としてハードディスクドライブ等の保存装置を有する通常のパーソナルコンピュータ等が使用される場合にはこれらの不正使用問題が生じる可能性が大きい。このような問題に対処するために、本発明者が既にＵＳ０８／４１６０３７（ＥＰ６７７９４９Ａ２）で提案している著作権管理プログラム及びデータコンテンツの再暗号化を採用することが有効であり、その場合に再暗号化等の処理を行う著作権管理プログラムを他のアプリケーションプログラムに優先させることが可能なリアルタイムＯＳあるいはエンベデッドシステムと呼ばれる構成とすることにより、不正使用の問題を適切に回避することができる。

【図面の簡単な説明】
【図１】　データ管理システム実施例の構成図。

33

【図２】　オブジェクトである複数のデータコンテンツを利用しての新しいデータコンテンツを作成する説明図。

【図３】　データ管理システムの他の実施例の構成図。

【図４】　データコンテンツ流通システムの実施例概要構成図。

【図５】　データコンテンツ流通システムの他の実施例の概要構成図。

【図６】　データコンテンツ流通システムのさらに他の実施例の概要構成図。

【図７】　加工シナリオ流通システムの実施例の概要構成図。

34

＊【符号の説明】

１，２，３，１１　データベース

４，５，６，７，１３，１９　ユーザ端末装置

８　著作権管理センタ

９，１４　通信回線

１０，１７，１８　記録媒体

１２　鍵管理センタ

１５，１６，ＩＰ　情報提供者

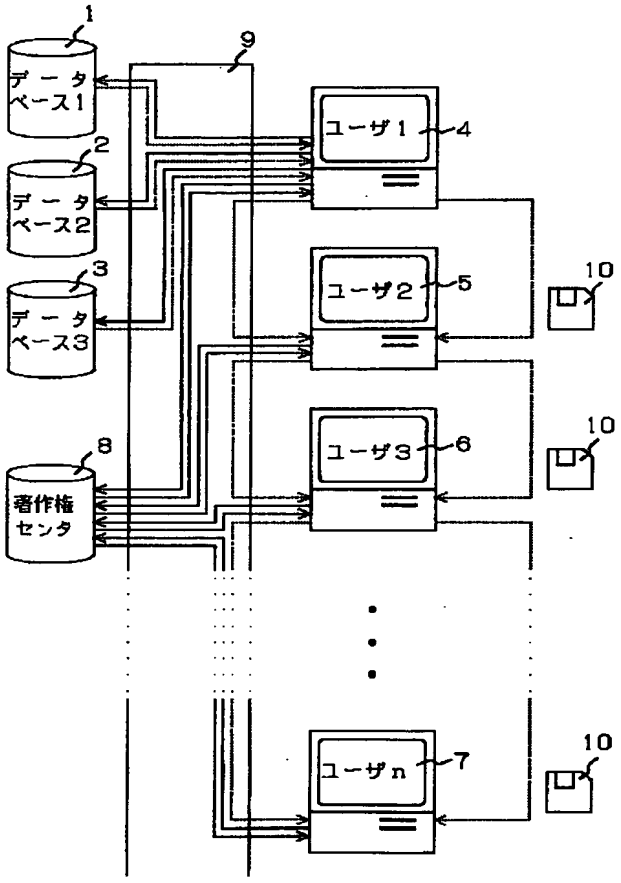
Ａ　著作権者

10　Ｕ1，Ｕ2，Ｕ3　ユーザ

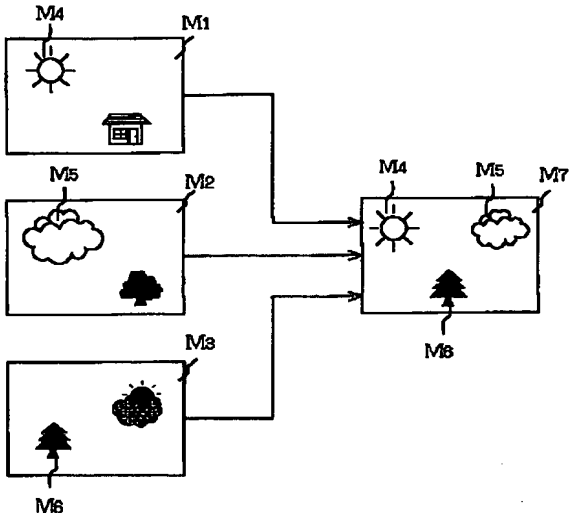
Ｅ　データコンテンツ加工者

＊　Ｄ　加工シナリオ販売者

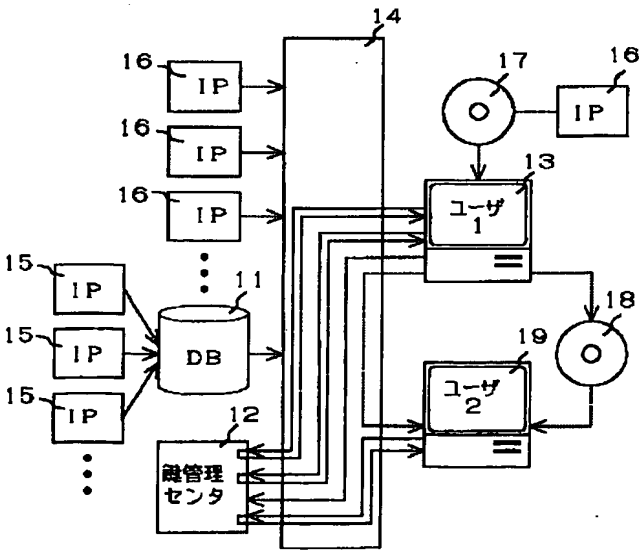
【図１】



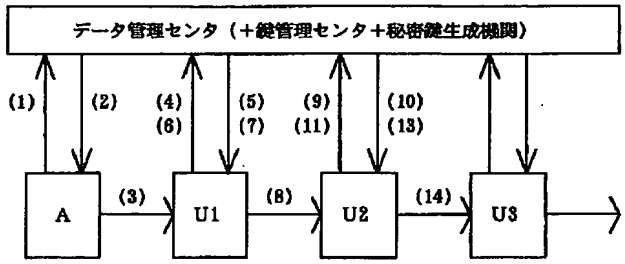
【図２】



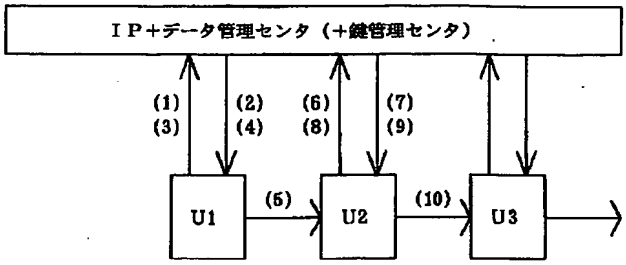
【図３】



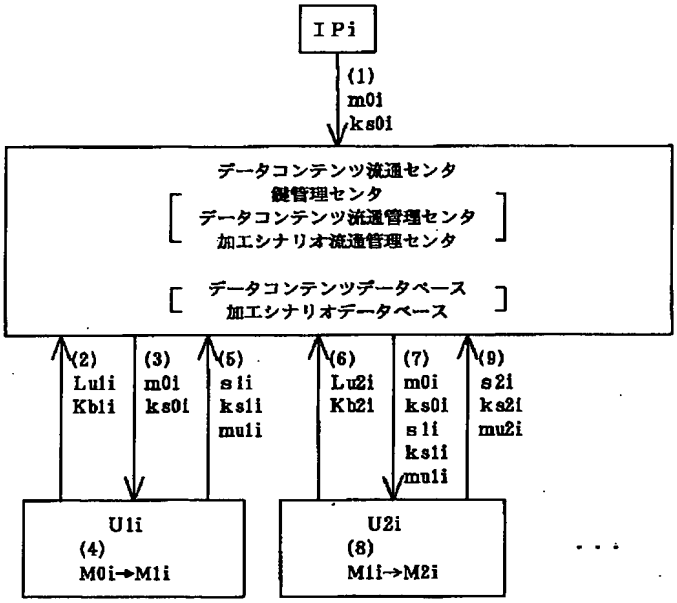
【図４】


データ管理センタ（＋鍵管理センタ＋秘密鍵生成機関）
(1)
(2)
(4)
(6)
(5)
(7)
(9)
(11)
(10)
(13)
A
(3)
U1
(8)
U2
(14)
U3

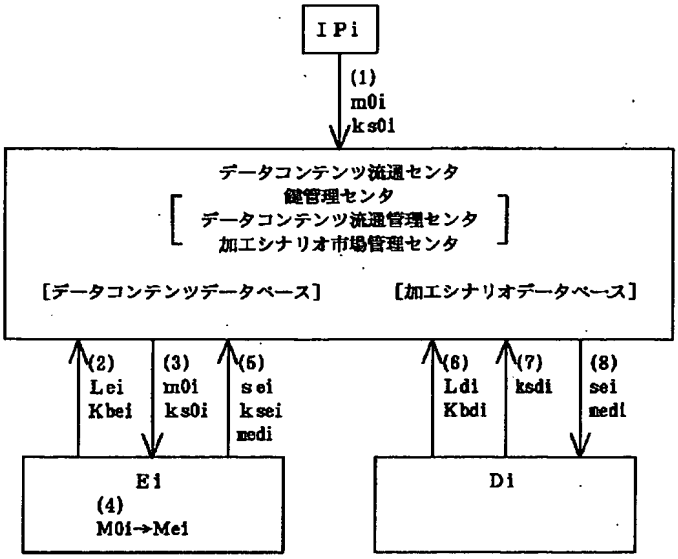
【図５】


ＩＰ＋データ管理センタ（＋鍵管理センタ）
(1)
(3)
(2)
(4)
(6)
(8)
(7)
(9)
U1
(5)
U2
(10)
U3

【図６】


ＩＰi
(1)
m0i
ks0i
データコンテンツ流通センタ
鍵管理センタ
データコンテンツ流通管理センタ
加工シナリオ流通管理センタ
データコンテンツデータベース
加工シナリオデータベース
(2)
Lu1i
Kb1i
(3)
m0i
ks0i
(5)
s1i
ks1i
mu1i
(6)
Lu2i
Kb2i
(7)
m0i
ks0i
s1i
ks1i
mu1i
(9)
s2i
ks2i
mu2i
U1i
(4)
M0i→M1i
U2i
(8)
M1i→M2i
・・・

【図７】



フロントページの続き

(51) Int. Cl.[6]	識別記号	ＦＩ
		Ｈ０４Ｌ　9/00　　６０１Ｂ